# Centralized Execution, Decentralized Chaos

## How the Air Force Is Poised to Lose a Cyber War

1st Lt John Cobb, USAF*

> *One victory [Operation Desert Storm] has swept all problems under the rug—the US's unchallenged lead in modern weaponry and technology has concealed the fact that their organization and strategy are obsolete, having failed to keep up with their technology.*
>
> —Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*

In the current state of cyber warfare, massive centralized networks are at best fragile and often indefensible.[1] The Air Force's network operations (AFNETOPS) paradigm relies on centralized control of the service's cyberspace; although arguably adequate for maintenance and counterintelligence in "cyber peacetime," it could fail spectacularly if ever tested by a serious cyber attack.

At present, the Air Force relies on a handful of units from the 67th Network Warfare Wing (67 NWW) to handle most aspects of network defense.[2] Primarily brought on by reductions in manpower, this consolidation also came about because of the perceived benefits accrued from establishing unity of command across Air Force cyberspace as well as reducing time-consuming training on network attack and defense tactics, techniques, and procedures. However, in seeking unity of command, the Air Force has almost completely abandoned decentralized execution, leaving its cyberspace vulnerable to a variety of attacks that could isolate base networks from the central network units. Compounding this problem is the fact that most Airmen remain unaware of these vulnerabilities, blindly assuming that enemy cyber attacks will never affect their own mission area. The current AFNETOPS paradigm must give way to a more effective model of network defense. Specifically, the service should take two steps to mitigate the risks of network failure and cross-domain mission failure: (1) cyber operators at the base level must be capable of running their networks and responding to attacks independently of higher-level network units, and (2) Air Force wings need to conduct exercises in which they operate under network isolation, degradation, and outage scenarios.

AFNETOPS includes units responsible for network operations and defense. Twenty-Fourth Air Force handles most aspects of Air Force cyberspace, including nearly all network administration. Within the Twenty-Fourth, the 67 NWW is responsible for most of the service's network defense. Within that wing, key network defense units include the integrated network operations and security centers (INOSC), the Air Force computer emergency re-

*The author is currently assigned to Headquarters Air University as officer in charge of the Information Engineering Branch. He previously served as officer in charge of network operations and of the Misawa Blue Team for the 35th Communications Squadron, Misawa Air Base, Japan.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| | | |
|---|---|---|
| 1. REPORT DATE<br>**2011** | 2. REPORT TYPE | 3. DATES COVERED<br>**00-00-2011 to 00-00-2011** |
| 4. TITLE AND SUBTITLE<br>**Centralized Execution, Decentralized Chaos: How the Air Force Is Poised to Lose a Cyber War** | | 5a. CONTRACT NUMBER<br>5b. GRANT NUMBER<br>5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | | 5d. PROJECT NUMBER<br>5e. TASK NUMBER<br>5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**Air and Space Power Journal,155 N. Twining Street,Maxwell AFB,AL,36112-6026** | | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | 10. SPONSOR/MONITOR'S ACRONYM(S)<br>11. SPONSOR/MONITOR'S REPORT NUMBER(S) |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT<br>**Approved for public release; distribution unlimited** | | |
| 13. SUPPLEMENTARY NOTES | | |
| 14. ABSTRACT | | |
| 15. SUBJECT TERMS | | |

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | **Same as Report (SAR)** | **6** | |

**Standard Form 298 (Rev. 8-98)**
Prescribed by ANSI Std Z39-18

sponse team (AFCERT), the 624th Operations Center, and the 26th Network Operations Squadron. Specifically, the two INOSCs have purview over geographic regions (INOSC East and INOSC West); they configure and operate core services across the base networks in their domain, responsible for most base boundary protection and network security devices (the INOSC runs most network-defense software tools and devices even though they might be physically present at the local base). AFCERT experts "diagnose and treat" viruses and other malware in network emergencies. The 624th Operations Center maintains situational awareness of Air Force cyberspace (including all major network defense issues) for Twenty-Fourth Air Force and other relevant commanders. Finally, the 26th Network Operations Squadron has networkwide oversight and security responsibilities. For example, if base X is attacked by a virus, the INOSC will close down some of the network "entrances and exits" (ports on the firewall) and try to repair any damage; AFCERT will help identify the attack and provide countermeasures; and the 624th Operations Center will coordinate and update commanders on the situation.

Most core network services across the entire Air Force are controlled by these centralized network-operations facilities. Although base-level technicians can control many routine functions such as modifying accounts or adding new machines to the network, only the off-site 67 NWW personnel can deal with major issues and changes because base-level administrator accounts are not configured to allow local technicians to modify core services or servers.[3] Since 67 NWW detachments typically reside at only one base per major command, they rely on functioning links between bases to carry out their mission.[4] In the latest construct, base-level network technicians are somewhat analogous to gas station attendants who can wash and refuel cars but lack the equipment to perform major repairs. Applying this centralized on-call approach to network defense assumes that repair teams can reach the least accessible station to help a customer whose "vehicle" has been damaged by attackers. Additionally, this construct leaves distant stations underprepared when attackers target access roads, preventing repair teams from arriving to help the stranded customer.

When the Air Force's network infrastructure is not under attack, centralized network service causes some frustration but works reasonably well (and, arguably, saves money and manpower compared to possible alternatives). However, in the face of a serious cyber attack, this model will break down. The AFNETOPS construct is the epitome of centralized execution, with attendant operational weaknesses such as unresponsiveness to local commanders, delays in approving and implementing changes, and difficulty adapting standardized equipment and practices to unique locations. Worse, it leaves base networks paralyzed if they become isolated from higher-tier units (or, specifically, higher-level administrator accounts).

How likely is such isolation? In cyber warfare, it is virtually inevitable. The Air Force leases from private telecommunication companies most of the "circuits" that connect bases, and these circuits are vulnerable to distributed denial of service (DDoS) attacks from hostile botnets. (The network equivalent of radio jamming, botnets are collections of thousands to millions of hijacked computers that hackers use to attack a target simultaneously.)[5] Nor are these leased lines the only weakness—DDoS attacks can also target the firewalls and routers where Air Force networks connect to the outside world. As demonstrated by the Internet isolation of Estonia in 2007, technology does not always allow a quick response to major DDoS attacks against the long-haul links between physical locations (especially at key bottlenecks such as transoceanic cables).[6] To be fair, defenses against DDoS attacks exist (often variations on blocking traffic from parts of the Internet or the entire Internet), but they are not foolproof.[7] A capable cyber foe will not limit his

attacks to a mere isolated portion of otherwise functional base networks.

DDoS attacks represent only one method of undermining a base network; the Air Force's network hierarchy is also vulnerable to simpler cyber attacks. An enemy could easily target our vulnerabilities and thereby degrade networks—either in preparation for a DDoS attack or in lieu of one. If a foe can infect a handful of computers with viruses—even simple, crude ones—he can cripple a network just by overloading it with more traffic than the network can handle. (This sort of denial of service differs from a DDoS, in which the overload originates outside the victim network and usually targets boundary devices connecting the victim network to the Internet.) This type of denial-of-service attack, usually involving phishing techniques to implant the viruses, requires some skill to evade network defenses and is difficult to perform successfully if all computers on the network are receiving correct updates and patches.[8] Unfortunately, both state and criminal hackers quite commonly have the skill to launch denial-of-service attacks, and most Air Force networks (including those maintained by the author) include machines weeks to months behind on the required updates.[9] Often, the most important machines are the least secured since technicians worried about patches breaking their logistics or scheduling database sometimes refuse needed security updates for months. Regardless of the criticality of the machines, infecting a few of them so that they begin "spewing traffic" (i.e., sending large amounts of data across the network) will quickly overwhelm the base network. Past base-network security exercises suggest that even the most poorly crafted phishing attacks find a few victims, while more sophisticated attacks can prove devastatingly effective.[10]

The necessary permissions (administrator accounts), training, and practical experience needed to respond to attacks now reside only within the units of the 67 NWW.[11] If, however, an attack has saturated a base network (i.e., the infected computers are sending so much data that no one can establish a connection with machines on the victim network), outside administrators will find themselves powerless to assist. Every network has bottlenecks and choke points: devices that can handle only so much data per second, authentication servers that can accommodate only a few thousand connections at a time, and security devices that block traffic when their queue of packets to inspect is too long. When these points reach saturation level, parts of the base network become cut off from each other and the outside world. The tools used by network technicians (at all levels) to maintain and repair their networks will then fail, unable to connect with distant computers (whether across a continent or across the street). Depending on the number of machines infected, the effects of the attack could range from a few buildings unable to connect to the network to most of the base populace unable to log in. In the more serious cases, technicians can resolve the problem only by physically removing infected machines for repair. Since modern network maintenance is predicated on fixing most issues remotely, physically finding and repairing infected machines can require days or even weeks—assuming that local technicians have the right tools to recover from the attack once they find the machines.

The aforementioned cyber attacks are relatively easy to perpetrate, conducted by a lone hacker or a small group working in concert. A country with a more robust cyber warfare program can unleash much more sophisticated attacks, potentially capable of controlling or even destroying significant numbers of machines on the network. A typical month uncovers more than a dozen security flaws in the software used by standard Department of Defense computers.[12] An attack based on one of these weaknesses before release of the patch could spread for hours or even days before technicians could stop it. Potentially, such an attack could cause a network outage lasting days or weeks, depending on the level

of damage and the scope of the attack (local or worldwide).[13]

If these more sophisticated attacks, carried out on behalf of state actors, are likely in any cyber war—and future conflicts almost certainly will include both cyber and kinetic battles—then what preparations can we make?[14] We must take two important steps to mitigate the impact of such attacks on Air Force cyberspace. First, we need to discard the current AFNETOPS paradigm, which assumes that centralized experts will deal with attacks during wartime. These experts will be swamped and cut off from most of the bases needing their help. Technicians at the base level require training and experience to deal with major attacks when the base becomes isolated; moreover, they must have access to administrator accounts with enough privileges to act as "cyber first responders" to an attack without relying on the 67 NWW's experts for assistance. Second, the Air Force should learn how to operate during network degradation and outage.

There are ways to give base-level technicians the tools and training they need without disrupting the cyber chain of command. For example, encouraging base communications units to maintain small training or exercise networks offers a feasible way of improving base-level technicians' skills. The Air Force should ensure that each base maintains a few dozen network devices and computers with configurations approved by the 67 NWW; these systems could simulate and defend against threats—possibly with the assistance of intelligence or aggressor units. Serving as "cyber flight simulators" for network first responders, they would give base-level technicians critical practice in dealing with local threat scenarios and operating a network when higher-level support is cut off. In addition, even though giving these technicians too much control over their network may threaten unity of command, in emergencies they need access to administrator accounts that give them full control over their base network. This access should not be used—or even available—during routine operations, but it is essential that these accounts exist for use in responding to attacks. Finally, the Air Force should consider high-level training in network defense for significant numbers of key base-level technicians so they can deal with these attacks. Although doing so may prove expensive, the status quo is not sufficient to defend Air Force cyberspace. If the service is serious about AFNETOPS, it must provide base network defenders with the training and experience to use their tools effectively; otherwise, networks will remain vulnerable, regardless of who possesses administrator accounts. The Air Force must correct the serious vulnerabilities in the AFNETOPS structure, mentioned earlier, that threaten to cut off base networks from the network hierarchy. By letting some network functions devolve to base-level technicians in emergencies and by ensuring that those personnel have enough training to use these tools, we can greatly enhance the survivability of Air Force cyberspace.

Ultimately, such survivability is important because of the missions it enables across all domains. Whether network failure occurs via loss of an air operations center's situational awareness tools, collapse of just-in-time logistics, or delays in base alert systems, it leads to rapid decline in the effectiveness of most Air Force units.[15] Consequently, not only network technicians but also ordinary Airmen should adjust their habits to prepare for cyber warfare by adapting and learning to operate when their base network comes under attack. Even when local technicians can fix the worst of the damage, hours or (more likely) days will pass before the network resumes normal operating status. The Air Force trains its pilots to perform tactically without communications, yet few of its wings offer training on how to handle network isolation, degradation, or outage at the operational level. Individual wings (especially flying wings and equivalent units) must correct this omission by periodically assessing their ability to operate in the face of realistic cyber attack. This may entail simulating sys-

tem outages, configuring a network so that a sham virus takes certain machines offline, mimicking a communications blackout for hours or days, or working with corrupted systems. Although putting an entire wing on an exercise network and having an aggressor unit launch actual cyber attacks may prove unrealistic, most base communications squadrons can simulate the effects created by those cyber attacks. By practicing the projection of airpower over multiple days while dealing with little or no network access, wings can prepare for future conflicts that will likely include disruptive cyber attacks.

Because major cyber attacks will soon become a common part of war, the Air Force must adjust accordingly to maintain national security in this new environment. By reducing overcentralization of the current AFNETOPS structure and by training all Airmen to perform their mission despite network damage, we can reduce the impact of cyber attack and ensure that network degradation does not produce catastrophic mission failures. In sum, both users and network technicians need to prepare for cyber war and understand the accompanying demands and limitations they will face. ✪

*Maxwell AFB, Alabama*

## Notes

1. See Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: People's Liberation Army Literature and Arts Publishing House, February 1999). (Author's translation, with assistance from Man Tsang.) For an English translation of the full text, see "PLA Colonels: 'Unrestricted Warfare': Part I," in "Chinese Doctrine," Federation of American Scientists, http://www.fas.org/nuke/guide/china/doctrine/unresw1.htm. Written in response to Operation Desert Storm and the US shift to network-centric warfare, *Unrestricted Warfare*—a classic of modern Chinese military theory—discusses ways that China (and its peers) can negate US advantages in technology and tactics via various asymmetric strategies. Although not all of its predictions have come to pass, the work was in many ways visionary, representing one of the first Chinese texts to deal with cyber warfare.

2. Air Force doctrine defines *computer network defense* as "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense [DOD] information systems and computer networks." Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 15 July 2010, 52, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf. Note that the cyberspace operations lexicon recently released by Gen James E. Cartwright, USMC, uses the term *cyber defense*; for most purposes, the terms are interchangeable. "Joint Terminology for Cyberspace Operations" (Washington, DC: Joint Staff, [November 2010]), 6, http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

3. The term *base-level technicians* refers to maintainers of the local base network—typically members of the base communications squadron, often those in positions such as network operations / network control center, communications focal point, cyber surety, or cyber transport. This article uses *local* and *base* interchangeably to describe these Airmen, and *administrators* and *network technicians* to refer to the Airmen who run and maintain networks. For the sake of simplicity, this discussion omits the roles of units of the Defense Information Systems Agency, now part of US Cyber Command. Some of the actions attributed to the 67 NWW are actually performed by Cyber Command units (usually requested and coordinated by 67 NWW personnel). Typically, those units are as centralized as those of the 67 NWW, and the problems described in this article are the same, regardless of which unit's network operations and security center is in charge. Chapter 2 of AFDD 3-12, *Cyberspace Operations*, describes the basics of the relationship.

4. For historical reasons, each major command generally has an INOSC detachment handling the more routine aspects of core network services across the command.

5. Some experts speculate that recent attacks attributed to North Korea were tests of this type of attack. See Elinor Mills, "Report: Countries Prepping for Cyberwar," *CNET*, 16 November 2009, http://news.cnet.com/8301-27080_3-10399141-245.html. For a more skeptical analysis of that attack, see Kim Zetter, "Lazy Hacker and Little Worm Set Off Cyberwar Frenzy," *Wired*, 8 July 2009, http://www.wired.com/threatlevel/2009/07/mydoom/. According to P. W. Singer, the DOD leases 95 percent of its communication links from commercial providers, adding an extra layer of complexity to any response. See his book *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Books, 2009), 200.

6. During the DDoS attacks against Estonia in 2007, which lasted for weeks, major banking and government systems were down for hours, and most Estonian networks were cut off from the rest of the world for several days. See Clark Boyd, "Cyber-War a Growing Threat Warn Experts," BBC, 17 June 2010, http://www.bbc.co.uk/news/10339543.

7. For a discussion of related issues, see Richard A. Clarke and Robert K. Knake, *Cyberwar: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 179–218.

8. "Phishing" refers to e-mails sent with malicious intent and modified to appear to come from a trusted person, firm, or unit. Whereas in the DOD's usage, phishing includes deceptive e-mails that install viruses, many other authorities limit the practice to deceptive messages that perform identity theft. For more information, see *Wikipedia: The Free Encyclopedia*, s.v. "phishing," http://en.wikipedia.org/wiki/Phishing.

9. For an overview of what less-experienced hackers are capable of with popular tools, see "Metasploit Express," noobz Network, 5 June 2010, http://www.n00bz.net/metasploit-express/. Note that experienced criminal hackers have capabilities far beyond these, and state-sponsored groups tend to surpass everyone else. At a recent conference, Lt Gen William T. Lord, the Air Force's chief information officer, observed that " 'we have over 19,000 (information technology) applications in the Air Force,' . . . noting that Electronic Systems Center's IT Center of Excellence at Maxwell Air Force Base-Gunter Annex, Ala., examined about 200 of them. 'All of them had over 50 vulnerabilities.' " Chuck Paone, "General Calls for Network Utility, Security Balance," AF.mil, 17 August 2010, http://www.af.mil/news/story.asp?id=123218114.

10. For a slightly less anecdotal example of the effectiveness of poorly crafted phishing, see John Timmer, "Users Are Still Idiots, Cough Up Personal Data Despite Warnings," *Ars Technica*, http://arstechnica.com/science/news/2010/08/users-are-still-idiots-cough-up-personal-data-despite-warnings.ars. This article uses the word *virus* in a general sense to describe all malware (malicious software); in fact, the attack described would use a combination of viruses and worms.

11. For more details, see "67th Network Warfare Wing," 24th Air Force, http://www.24af.af.mil/units.

12. In August 2010, Microsoft released fixes for 14 security flaws in the Windows operating system; this figure does not include security issues with other software such as Adobe Acrobat or Java. See "Microsoft Security Bulletin Summary for August 2010," Microsoft TechNet, 1 September 2010, http://www.microsoft.com/technet/security/bulletin/ms10-aug.mspx; and Emil Protalinski, "Patch Tuesday: Microsoft's Most Security Bulletins Ever!," *Ars Technica*, http://arstechnica.com/microsoft/news/2010/08/microsoft-patch-tuesday-for-august-2010-14-bulletins.ars.

13. Given the limited number of experienced network defense technicians, 67 NWW units might be forced to address issues one or two bases at a time within their area of responsibility, even after attacks have been brought under enough control that the bases are no longer isolated. If it takes multiple days to repair each base, then bases at the end of the list could face weeks of network degradation.

14. Even countries as "off-line" as North Korea have established cyber warfare programs. See Dan Raywood, "North Korean Cyber Warfare Unit Strengthened with Recruitment of 100 Hackers," *SC Magazine*, 6 May 2009, http://www.scmagazineuk.com/north-korean-cyber-warfare-unit-strengthened-with-recruitment-of-100-hackers/article/136235/; and Clarke and Knake, *Cyberwar*, 27. The deputy secretary of defense has stated that "more than 100 foreign intelligence agencies" target DOD networks. The tools and skills used in cyber espionage are largely identical to the ones needed for cyber attacks. See William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97–108; and Bruce Schneier, "Cyberwar," *Schneier on Security* (blog), 4 June 2007, http://www.schneier.com/blog/archives/2007/06/cyberwar.html.

15. For a discussion of vulnerabilities similar to those of situational awareness tools, see Clarke and Knake, *Cyberwar*, 170–73.